E29 P143PCT AB/ej 2003-10-24

Title:
ARRANGEMENTS AND METHODS RELATING TO SECURITY IN NETWORKS
SUPPORTING COMMUNICATION OF PACKET DATA

FIELD OF THE INVENTION
The present invention relates to a system for enhancing security of end user station access to Internet and intranet, e.g. corporate access, over an access network with access points, which system comprises gateway packet data nodes and packet data support nodes. The invention also relates to a packet data support node for enhancing security at end user station access to Internet and intranets, e.g. so called corporate access. Still further the invention relates to a node in a mobile communications system supporting communication of packet data comprising security indicating means for providing access points with a security indication to allow for secure remote access connections to corporate networks. Still further the invention relates to a method for enhancing security for end user station access to Internet and intranets, e.g. so called corporate access.

STATE OF THE ART
In the global communications society of today, in which end users often move from one place to another but still need to be able to access Internet as well as one or more intranets, e.g. the company intranet, there is a need for, particularly on behalf of companies but for commercial reasons also for operators of communication systems, to be able to offer means for enabling remote access to corporate networks. This can be done in different manners, for example over GPRS, WLAN etc. However, for the provision of access to an intranet it is of utmost importance, a precondition, for making the service successful, that security can be upheld and

2

guaranteed since the security aspect in such cases generally is very high and exceedingly important.

For corporate access using GPRS, for example, a serious security loophole has been identified. This relates to the case when multiple Primary PDP Contexts are active. This may, actually have as an effect that the loophole makes the user station or user equipment (IE) act as a router for packets between the connections created by the different PDP contexts. Among others there has been a suggestion (by Vodafone, cf. S2-032979, CR (Change Request) 434 on 3GPP 23.060, Brussels 18-22 Aug. 2003) in order to reduce the impact of such a loophole, by removing the ability to have connections to public access and certain private APNs (Access Point Names) simultaneously. A similar security issue relating to a user equipment having multiple concurrent Primary PDP Contexts active is also relevant for situations wherein multiple connections are possible, among others including circuit switched connections, packet switched connections, WLAN connections etc. The risk for abusive access comes from unauthorized third parties hacking or manipulating a user terminal in order to be able to access another network, particularly an internal company network or an intranet. For GPRS services, the issue is to some extent handled in 3GPP TS 23.060, stating that the use of radio communications for transmission to/from subscribers in mobile networks makes them particularly sensitive to misuse of the resourses by unauthorized persons using manipulated user stations (UEs). In order to protect the system, access control can be implemented, i.e. the network can support restrictions on access by or to different GPRS subscribers, such as restrictions by location, screening lists, and so on. However, so far there is no satisfactory mechanism to provide for such protection, not to speak from even better protection.

The solution referred to above has to somehow be enforced in for example a packet data support node such as SGSN, but still there is no satisfactory solution as to how such an enforcement should be achieved.

5

It has been suggested that certain APNs, such as corporate APNs, be security marked, i.e. that the APN is subject to a raised security level. This could be provided for by configuration of an APN restriction, it is hereby referred to the above mentioned

10 document S2-032979, CR on 23.060 "Security Issue with Multiple PDP Contexts", in the GGSN.

An APN restriction as referred to above is then transferred to the (e.g.) SGSN where the security is to be enforced. The APN

15 restriction needs to be configured in GGSN for example, and enforced in SGSN in order to function in a roaming case, as well as when subscribers of particular operator visit other networks operated by other operators. The transfer between SGSN and GGSN is suggested to be carried out through the addition of the parameters

20 APN restriction and maximum APN restriction to be transferred in create PDP context requests and update PDP context requests. It should also be a feature to perform calculation/decision as to whether certain APN combinations are permissible in the PDP context activation and inter-SGSN Routing Area Update procedures.

25

However, a solution as suggested above only solves part of the problem. One example of a situation for the problem is not solved, is when a Laptop uses GPRS for corporate access. It may in principle at the same time have simultaneous connections to for

30 example Internet using other links of access, for example fixed access or access over WLAN.

Suggestions have also been made relating to the use of firewalls/VPN clients in a user terminal in order to solve this problem. However, there is also a need for a network based solution to the problem and not only a terminal based solution,

5   for example in order for operators to be able to claim that their network is secure. In addition thereto it is desirable to be able to provide for a secure remote corporate access, in a particular case over e.g. GPRS. The conclusion also must be that it is not sufficient to exclusively use terminal based security mechanisms

10   but that network-based security mechanisms and terminal-based security mechanisms are complementary. Both contribute to provide a sufficient level of security to handle different security attacks. Network-based security mechanism provide for protection when an end user uses the wrong terminal type, has failed to

15   setup, has misconfigured or does not want to use appropriate terminal-based security mechanisms. Terminal-based security mechanisms, on the other hand, protect from threats which network-based mechanisms are unable to detect. Network-based security solutions have the advantage that they are easier to combine with

20   an operator service offerings. It gets possible to setup agreements between operator and for example an enterprise for, on the user end, put into effect of such network-based security mechanisms.

25   Thus, the problems with multiple PDP contexts and the risk that a user station, particularly a user equipment UE, be used as a router to get access from Internet to corporate intranets, needs to be solved. Generally a compromised or manipulated user equipment can not be trusted to perform necessary actions to

30   satisfactorily safeguard the system. Even if firewalls are used, this may be insufficient, and e.g. if the firewall is located in an endpoints network and the network is accessed via a dedicated APN, a user station allocated a valid IP address for that APN will

always be able to pass through the firewall. Attacks thus may appear to the firewall as entirely normal access actions. It is often also not practical to install firewall software in the user station for different reasons, e.g. limited processing power and
5   multiple channel equipments connected to a single mobile terminal etc. Therefore it seems exceedingly important to find a network-based access control solution which provides a satisfactory degree of security and it is of course attractive both to operators of systems as well as to the end user or companies, for which it is
10   exceedingly important that third parties can not access their networks.

SUMMARY OF THE INVENTION
What is needed is therefore a system as initially referred to
15   through which a user can be provided with access to corporate networks, e.g. over GPRS etc. in a secure manner. A system is also needed through which an operator can provide a user with such access in an easy, reliable and secure manner. Particularly a system is needed which provides a network-based solution. Still
20   further a system is needed allowing GPRS, or any 3GPP system (or WLAN) to provide remote corporate access in a secure and reliable manner. Particularly a system is needed through which it gets possible to control which, if any, connections to public access and private intranets can be provided simultaneously, i.e. through
25   which it is possible to control which simultaneous connections that are acceptable while still providing for a satisfactory degree, or the desired degree, of security for a particularly corporate access, or for each individual access point connections.

30   It is particularly an object of the invention to suggest a system through which it gets possible to enforce a security mechanism through which one or more of the above mentioned objects can be achieved. Still further it is an object of the invention to

provide a solution to the problem when several access point connections, e.g. when several PDP contexts, are active while still providing for the desired degree of security for each access point connection. It is a particular object of the invention to

5   suggest a system through which the risk can be eliminated that a user station, e.g. a user equipment UE, acts as a router for packets between connections created by the PDP contexts, when there are several access points connections, or PDP contexts.

10   It is a particular object to provide a system through which the risk of abuse by a third party for getting access to a corporate network can be eliminated or avoided to the largest possible extent.

15   It is also a particular object of the invention to provide a system through which the problems associated with the enforcement at a security mechanism whilst a roaming situation, e.g. relating to a user changing networks, e.g. visiting other networks, can be solved.

20

It is a particular object of the invention to protect corporate networks when a user of for example a Laptop uses several access networks or several access techniques, e.g. access over GPRS, fixed access and access over a WLAN.

25

Further yet it is an object of the invention to provide a system through which reliable corporate access can be provided, particularly while also supporting mobility. It is also a particular object to provide a system through which secure

30   corporate access can be provided in a manner which is as easy as possible, particularly without requiring extensive protocol changes.

A packet data support node for enhancing security of end user
station access to Internet and intranet(s), e.g. corporate access,
is also needed through which one or more of the above mentioned
objects can achieved. Still further a node in a mobile
5   communication system supporting communication of packet data
comprising security indicating means for providing access points
with a security indication, to allow for secure remote access to
corporate networks, is needed, through which one or more of the
above mentioned objects can be met.

10

It is also an object of the invention to provide a method for
enhancing security at end user station access to Internet and
intranets, e.g. at corporate access, through which method one or
more of the above mentioned objects can be achieved.

15

Therefore a system as initially referred to is provided having the
features of the characterizing part of claim 1. Therefore also a
packet data support node is suggested which has the characterizing
features of claim 19. Still further a node in a mobile
20   communications system is suggested which has the characterizing
features of claim 31. Still further a method is provided having
the characterizing features of claim 37.

Advantageous and alternative embodiments are given by the appended
25   subclaims.

BRIEF DESCRIPTION OF THE DRAWINGS.
The invention will in the following be further described, in a
non-limiting manner, and with reference to the accompanying
30   drawings, in which:

Fig. 1A   shows   a   first   implementation   wherein   security
provisioning and distribution is performed in a GGSN
node whereas enforcement is performed in SGSN,

5   Fig. 1B   shows   a   second   implementation   in   which   security
indication provisioning and distribution is performed
in a Domain Name Server (DNS), whereas enforcement is
performed in a SGSN,

10   Fig. 1C   shows   a   third   implementation   in   which   security
indication provisioning and distribution is performed
in a Home Location Register (HLR) whereas enforcement
is performed in a SGSN,

15   Fig. 2A   illustrates in a more detailed manner the embodiment in
which security indication provisioning and distribution
is provided by a GGSN,

Fig. 2B   illustrates in a more detailed manner an implementation
20   in which security provisioning and distribution is
provided by a DNS,

Fig. 2C   illustrates in a more detailed manner an embodiment in
which security indication provisioning and distribution
25   is provided for by a HLR,

Fig. 3   schematically illustrates a first implementation of
enforcement based on a dynamic protection mechanism,

30   Fig. 4   schematically illustrates a second implementation of
enforcement based on a static protection mechanism,

Fig. 5A   is a sequence diagram illustrating the procedure when a
             GGSN is used for security indication provisioning and
             distribution,

5   Fig. 5B is a sequence diagram illustrating the procedure when a
             DNS is used for security indication provisioning and
             distribution,

Fig. 5C   is a sequence diagram as in Fig. 5A, 5B wherein a HLR
10   handles provisioning and distribution of security
             indications,

Fig. 6A   is a flow diagram illustrating a dynamic enforcement
             mechanism according to Fig. 3 when a packet is incoming
15   to a security indicated access point,

Fig. 6B   illustrates, for the dynamic enforcement mechanism of
             Fig. 6A, when a packet is incoming to an access point
             which is not security indicated,

20
Fig. 6C   illustrates the timer controlled removal of a security
             indication,

Fig. 7   is a flow diagram describing a first implementation of
25   a static enforcement mechanism,

Fig. 8   is a flow diagram describing a second implementation of
             a static enforcement mechanism,

30 Fig. 9   is a flow diagram describing a third implementation of
             a static enforcement mechanism, and

Fig. 10   is a schematical flow diagram illustrating support of
           mobility management.

DETAILED DESCRIPTION OF THE INVENTION

5   Fig. 1 shows a first implementation of the inventive concept for
     providing secure remote access to a corporate network, corporate
     intranet 10 in this case. As can be seen access can also be
     provided to Internet 20, and unless the inventive concept is
     implemented, due to multiple PDP contexts a security loophole can
10   be said to exist as discussed in the first part of the present
     application. The user station US 1, e.g. a user equipment UE, is
     connected to an SGSN 2 (in more general terms a packet data
     support node) which is in communication with a first GGSN (Gateway
     GPRS Support Node) 3A for corporate intranet access, and to
15   another GGSN 3B for Internet access. It might however be one and
     the same GGSN. In this implementation the means for providing and
     distributing a security indication, 11, are provided in GGSN 3A
     with access point AP. The security indication provided in
     providing and distributing means 11 is provided to enforcement
20   mechanism 21 in SGSN 2. As referred earlier in the application the
     security indication can be of many different kinds, for example it
     may simply comprise a flag, it may comprise an entire data
     structure or any thing therebetween, it may simply indicate that
     an access point connection over the access point AP, with Access
25   Point Name APN$_c$, is, in this embodiment, security indicated to a
     SGSN 2 or rather to the enforcement mechanism 21 thereof. An
     access point connection is here supposed to comprise a PDP
     context. The security indication may comprise an attribute added
     to the PDP context. It may also include information about which
30   other access point connections (types) that will be allowable
     simultaneously with said access point connection (if any). A
     number of different alternatives are possible. In one
     implementation the provisioning and distribution of security

indications or security marks can be performed as described in the document referred to earlier in the application.

A secure PDP context, i.e. a PDP context incoming to a security
5   indicated access point AP with APNc is tunneled between GGSN 3A, SGSN 2 and the user station 1. In one particular implementation a GTP (GPRS Tunneling Protocol) tunnel is used between GGSN 3A and SGSN 2, for WCDMA a GTP tunnel is also used between SGSN and a Radio Network Controller (RNC) (not shown in this figure) whereas
10 a RRC (Radio Resource Control) tunnel is used between the RNC and the user equipment US 1. For the GSM case instead LLC (Link Layer Control) is used between SGSN and the user station 1. As a matter of fact, there is not one tunnel between GGSN and the user equipment, but a number of concatenated tunnels.
15

The enforcement procedure will be carried out in SGSN 2 and different ways of enforcing the security indication will be described below with reference to figures 3,4,6A-9.

20 Particularly a security indication, e.g. a security attribute, is provided per APN (Access Point Name), which is a logical name referring to the external packet data network and/or to a service that the subscriber wants to connect to. The APN is composed of two parts, namely the APN network identifier, which defines to
25 which external network the GGSN is connected, and optionally a request service requested by the user station. This part of the APN is mandatory. APN also comprises an APN operator identifier, which defines in which PLMN (Public Land Mobile Network) GPRS backbone the GGSN is located. The network identifier thus defines
30 the connection part in GGSN (on the side of the Gi interface) whereas the operator identifier identifies which GGSN that is concerned. APN is formatted as a domain name which is translated to an IP address, at least the operator identifying part, with the

12

use of a domain name server (DNS) which exists in all IP networks. The network identification part which is translated to a connection port on the Gi interface to the GGSN can also be said to, indirectly, correspond to a corporate intranet or a corporate
5   access network.

Fig. 1B is a figure similar to that of Fig. 1A, and similar reference numerals are used for corresponding components or nodes. However, in Fig. 1B the provisioning and distribution of security
10   indications is provided in a domain name server DNS 4 comprising a corresponding means 12 which thus distribute the security indication to SGSN 2, or rather to the enforcement mechanism 21 provided therein.

15   In another embodiment where a modified DNS server is used it may be used in the following way:
     The SGSN asks the DNS server to resolve the APN domain name. The DNS returns the IP address of the GGSN and a full security indication, as described above, to SGSN.
20
     Also in this embodiment different enforcement mechanism can be implemented by enforcement means 21. For DNS based distribution of security marks, the APN resolution done when access point connections, e.g. PDP contexts, are activated, can be altered to
25   either support a simple form of security indications or a complete form. The input to a DNS server 4 is always a domain name, and the normal (simple) output is always one or several IP addresses. For a complete form of security indications the DNS server needs to be modified or extended with a new type of records which can store
30   the complete security indication.

     According to one implementation DNS 4 is used as a centralized database for security indications, and it may, in one embodiment,

13

be used in the following way: in DNS 4 the IP address for a
security indicated access point, or a security indicated APN, is
set to be an invalid, but by SGSN 2 known IP address, e.g.
0.0.0.0. When thus a security enabled SGSN 2 encounters this IP
5   address, it knows that the access point, or here APNc, is security
indicated. In order to get the real IP address, the SGSN 2 then
issues a new DNS request using a slightly modified APN such as the
"secure"   introduced   into   the   original   APN   (for   example
companyxxxsecure.comcom.se@mnc001.   mcc046.gprs).   The   DNS   is
10   configured to translate this into the IP address to the GGSN 3A
that should have been received in the first request or to an IP
address and a complete security indication. A benefit with such an
arrangement is that an SGSN that is not upgraded to support this
security mechanism will never get (or "fetch") the IP address to
15   GGSN. Hence the corporate access will not be possible to access if
it is not safe. It is an advantage with DNS based security
indication and distribution that this implementation, and other
DNS based implementations, do not require any protocol changes.
Mobility is supported when a user station moves from SGSN 2 to
20   another SGSN by means of Inter SGSN Routing Area Update (ISRAU),
cf. Fig. 10 below.

In implementations in which GGSN is used for provisioning and
distribution of security indications, the GTP protocol (and/or any
25   other relevant protocols) need to be modified.

Fig. 1C illustrates still another implementation for provisioning
and distribution of security indications. Like reference numerals
are used for corresponding elements or nodes as in Figs. 1A, 1B.
30   In this embodiment a Home Location Register HLR 5 comprises means
13 for provisioning and distribution of security indications,
which thus are provided to enforcement mechanism 21 in SGSN 2. HLR
based distribution of security indications comprises inclusion of

the security indications (e.g. APN restrictions) together with the
subscriber data from the HLR 5. When a subscriber (a subscriber of
an enterprise for example using GPRS based corporate access)
attaches to a GPRS/3G network, the security indication that is

5   configured into the HLR will be sent to SGSN 2. This is done using
the insert subscriber data message within the MAP protocol (Mobile
Application Protocol) or with equivalent messages. Alternatively
other protocols used to access the HLR or HSS, Home Subscriber
Server, which is an extended HLR for new services such as IMS, IP

10 Multimedia Subsystem, (for example Diameter or Radius protocols)
could be used. Mobility will also here be supported since the
security indication is forwarded to other SGSNs as a part of the
ISRAU procedure. This is done using the SGSN context response
message within the GTP (GPRS Tunneling Protocol) (cf. Fig. 10). It

15 is an advantage of HLR based security indication provisioning and
distribution that mobility will be supported and it is to a large
extent in line with the current 3GPP architecture. However,
protocol changes are required in MAP and GTP, and the HLR needs to
be modified. Like in the implementations described with reference

20 to Figs. 1A and 1B, any enforcement mechanism as will be described
below can be implemented.

Fig. 2A is a block diagram describing an embodiment as
schematically illustrated in Fig. 1A in which a GGSN 3A is used

25 for provisioning and distribution of security indications. In this
particular implementation is illustrated a GGSN 3A, an SGSN 2 and
an SGSN$_v$ 2'. The second SGSN$_v$ 2' is only illustrated to show how
mobility can be supported, i.e. when a user station moves from one
SGSN to another SGSN, and it is of course not necessary for the

30 functioning of the basic concept of the present invention.

GGSN 3A here comprises security indicating (S-I) storage 11A for
storing security indications, which is in communication with the

15

distribution means 11B supporting a conveying protocol communicating with protocol handling means 31 of SGSN 2. SGSN 2 comprises an enforcement mechanism 21 which may support dynamic or static enforcement of the security protection. In this figure

5   enforcement mechanism 21 is illustrated as external to the PDP context handler, 22, but it may as this well be included in the PDP context handler 22, as is illustrated in Fig. 2B which relates to an implementation in which a DNS is used for service provisioning and distribution. However, also when a GGSN 3A acts

10 or handles the security provisioning and distribution, the enforcement mechanism may of course be included in the PDP context handler 22, thus reducing the number of messages sent internally within SGSN 2. SGSN 2 also comprises one or more payload handlers 23, 23A, 23B. Of course only those blocks and

15 components which are of importance for the functioning of the inventive concept are illustrated in these figures for reasons of clarity. In these figures also are only illustrated that an enforcement mechanism is included, and they are silent as to whether it is static or dynamic. The security enforcement

20 mechanism 21 controls operation of the PDP context handler 22 and of the payload handler 23 (23A, 23B) by controlling which GTP tunnels that are to be setup or taken down (static case) or provides information to the payload handler as to whether packets can be sent or not (dynamic enforcement) and end point

25 establishment. Mobility is supported since all information relating to security indication in this security protection procedure can be transferred via the conveying protocol to another SGSN over Inter SGSN Routing Area Update (ISRAU). It is possible since the information is provided from an SGSN to

30 another, and not from a GGSN, in which case mobility would not be supported. SGSN 2' to which a user moves acts in a similar way as SGSN 2.

Fig. 2B is a figure similar to that of Fig. 2A but for the case
when the security provisioning and distribution is handled by a
Domain Name Server DNS 4. Thus, in this case the DNS 4 comprises
the security indication storage 12A and the distribution means 12B
5   supporting a conveying protocol communicating with conveying
protocol handling means of SGSN 2_1. Also in this case mobility is
supported by means of ISRAU to another SGSN, which however not is
illustrated specifically in this figure but which works similar to
the procedure described with reference to Fig. 2A. In the
10   embodiment illustrated in Fig. 2B SGSN 2_1 comprises one or more
payload handlers 23, 23A, 23B and a PDP context handler 22_1 but
the enforcement mechanism 21_1 is here included in the PDP context
handler. Of course, if DNS based security protection is
implemented, the enforcement mechanism could also be provided as a
15   separate enforcement mechanism externally provided in relation to
the PDP context handler 22_1. An advantage with an implementation
as described in Fig. 2B is that fewer messages are due to be sent
within SGSN 2_1. In other aspects the procedure is similar to that
described above with reference to Fig. 2A.

20

Fig. 2C shows another embodiment which is based on the use of a
HLR 5 for security indication provisioning and distribution, cf.
Fig. 1C. Also in this case mobility is supported as described with
reference to Fig. 2A. In this case however HLR 5 comprises a
25   security indication storage 13A, distributing means 13B comprising
a conveying protocol for communication with SGSN 2 over conveying
protocol handling means 31. SGSN 2 comprises an enforcement
mechanism 21, one or more payload handlers 23, 23A, 23B and a PDP
context handler 22 as described in Fig. 2A. Of course the
30   enforcement mechanism 21 might be included in the PDP context
handler 22 as disclosed with reference to Fig. 2B. In other
aspects the functioning is the similar to that described above.
Static and dynamic enforcement respectively will be further

17

described below with reference to sequence diagrams and flow
diagrams.

Fig. 3 schematically illustrates a first implementation of an
5   enforcement mechanism as provided in SGSN 2. This embodiment
relates to a dynamic security protection enforcement mechanism.
The dynamic security protection is activated when traffic is sent
on a PDP context to a security indicated access point. In Fig. 3
is illustrated a tunnel for APN_C, Corporate APN, and a tunnel for
10   an Internet APN, APN_I. SGSN 2 comprises an enforcement mechanism
21A comprising a detecting means 24A and means for dropping non-
security indicated access point connections 25A, particularly PDP
contexts. Here it is supposed that traffic on a security indicated
PDP context, I, is detected by detecting means 24A of the
15   enforcement mechanism 21A. When there is traffic on the security
indicated, or rather secure, PDP context, this will cause IP
packets to be dropped on all PDP contexts that are not secure, or
which are not security marked or which do not have the same
security marking or a security marking meeting some criterium or
20   criteria for allowing certain access point connections being
active or trafficated simultaneously. A PDP context to an APN_C can
be said to be secure, or provided with a security indication if
the access point or the APN is security indicated, if it is a PDP
context income to said access point having that APN when there
25   either are no other APNs active simultaneously or other security
indicated APNs for which the criteria coincide with those of the
first security indicated PDP context. Other non-secure or non-
criteria coinciding access point connections will be dropped. The
security indicated PDP context, or the PDP context(s) that are
30   allowed to be sent simultaneously, remain(s) activated for some
time which may be configurable by the operator after the last
packet has been sent. Then traffic will be allowed on all PDP
contexts again. In this case the packets of PDP context with APN_I

18

will be dropped until all the packets of PDP context - SI have been sent and when a given time interval has lapsed after sending of the last packet.

5   Fig. 4 is a schematical block diagram illustrating an SGSN 3 with an enforcement mechanism 21B comprising detecting means 24B and means for deactivating PDP contexts, 25B, i.e. not only dropping packets as in the case with a dynamic enforcement mechanism. In this embodiment a static enforcement mechanism is implemented.
10   Static security protection is activated when traffic is sent on a security marked PDP context, i.e. when a first PDP context is incoming to a security indicated access point or with a security marked APN, APNc. It may also be activated when a security marked PDP context is activated. Thus, when the detecting means 24B
15   detects traffic on APNc (a so called security indicated PDP context), this will activate the PDP context deactivating means 25B such that all PDP contexts that are not security indicated or do not have the same or a security indication fulfilling some given criteria such as to be allowable concurrently with the first
20   security indicated PDP context SI, these PDP contexts will be deactivated. Thus, as opposed to the preceding case with dynamic enforcement wherein the packets on non-secure PDP contexts only are dropped, here the PDP contexts are actually deactivated. This means that they have to be reactivated. Particularly lost PDP
25   contexts are reactivated manually by the user. Activation of new PDP contexts, or lost PDP contexts, is blocked as long as the security protection is active, e.g. until all traffic on a secure PDP context has been exchanged.

30   Three different algorithms can be implemented in a static enforcement mechanism, involving control before activation, control directly after activation and control after activation when a first packet is detected to a security indicated access

point, in other words a security marked PDP context. This will be
further discussed with reference to flow diagrams 7, 8 and 9
respectively.

5   Fig. 5A is a sequence diagram illustrating the inventive concept
in the case of GGSN based provisioning and distribution of
security indications. The sequence starts with the user equipment
UE sending an activate PDP context request to SGSN. It should be
clear that only messages of importance for the functioning of the
10   inventive concept are illustrated in Figs. 5A-5C. Thus, at
reception of the PDP context request from UE, SGSN sends a create
PDP context request to GGSN. In GGSN, which here is supposed to
handle security indication provisioning, a security indication is
added to the create PDP context response which is sent to SGSN. In
15   SGSN enforcement takes place as discussed above, and more
thoroughly with reference to the flow diagrams of Fig. 6-9
describing different ways to implement the enforcement. GTP
tunnels are used between SGSN and GGSN, and due to the
introduction of the security indication in the create PDP context
20   response, the GTP protocol has to be a modified due to the fact
that additional parameters are included. When security protection
has been enforced in SGSN, only payload which is secure is allowed
to/from the security indicated access point.

25   In the lower part of the figure is described how the sending of
payload to/from UE is affected when one or more security indicated
PDP contexts are active, i.e. after security protection has been
enforced in SGSN for an access point. If the user equipment wants
to send on secure payload (PL) to a security indicated access
30   point, this is blocked already at the user equipment since there
actually is no PDP context, as will be realized by an application
in the user equipment, in the case a static enforcement mechanism
has been implemented.

If on the other hand a dynamic enforcement mechanism is
implemented, insecure PL to a security indicated access point will
be sent from the user equipment, but it will be blocked in SGSN
5   which is responsible for dropping insecure payload, the PDP
contexts still existing. The secure payload in the direction to a
security indicated access point will be sent from UE via SGSN and
GGSN to the security indicated access point as intended.

10 On the downlink, from the security indicated access point insecure
payload will be blocked at GGSN in case the static enforcement
mechanism is implemented. Insecure payload will be blocked at SGSN
if a dynamic enforcement mechanism is implemented. The secure
payload from a security indicated access point will be forwarded
15 by a GGSN and SGSN to UE. By a security indicated access point is
here meant an access point of some equipment to a corporate
network. By an access point connection is here meant a tunneling
between a user station (e.g. UE) and a GGSN.

20 Fig. 5B is a sequence diagram similar to that of Fig. 5A, but for
the case when the provisioning and distribution of security
indications is handled by a DNS. It is here supposed that user
equipment UE sends an activate PDP context request to SGSN. SGSN
then sends a DNS query (for a domain name) to DNS, which is
25 security indicated and returns a DNS response to SGSN with a
predefined IP address which indicates security indication.
Enforcement then takes place in SGSN, either in a dynamic way or
in a static way. Subsequently SGSN sends a DNS query (domain name
with predefined extension) to DNS which returns a DNS response
30 with IP address to the concerned GGSN to SGSN. Thereupon SGSN
sends a create PDP context request to that GGSN. Sending of secure
and insecure payload respectively after enforcement in SGSN is
similar to the situation as described in Fig. 5A.

As an alternative the DNS response (the first or the second) may contain a complete security indication together with the requested GGSN address. If it is done in the first DNS response, the second DNS query and response are not needed.

Fig. 5C is a figure similar to Figs. 5A, 5B but for the case when the provisioning and distribution of security indications is handled by an HLR. In this case UE sends an attach to SGSN, which sends the message Update Location to HLR. When this is received, HLR, which comprises the security indications, returns the message Insert Subscriber Data including a security indication to SGSN. This is acknowledged to HLR via SGSN, and HLR returns an Update Location Acknowledgement to SGSN. The enforcement takes place in a SGSN in any appropriate manner as discussed above. PDP context activation messageing is then performed between UE and HLR using the GTP protocol. The sequence above between SGSN and HLR uses the MAP (Mobile Application Protocol) protocol which thus is modified in that additional parameters are introduced. GTP is also modified in that additional parameters relating to the security indication are introduced.

The uplink and downlink transfer or sending of payload is allowed/inhibited in a manner similar to that described with reference to Fig. 5A.

Figs. 6A-6C are flow diagrams schematically describing the procedure with a dynamic security protection enforcement mechanism on packet level.

It is supposed that dynamic security protection is implemented in an SGSN, and that the procedure starts, 100. It is then supposed that a packet is detected on a PDP context to a security indicated

access point, 101. Then it is examined if a security indication is already set, 102. If yes, the packet is forwarded, 104. If however no security indication is set, 102, the security indication (e.g. a flag) is set according to which all traffic on other PDP
5   contexts to the security indicated access point (exposing the security loophole) should be dropped, 103. In one implementation this security indication merely relates to all traffic on all other PDP contexts, whereas in other implementations some criteria may be included in the security indication, indicating which PDP
10   contexts to the same security indicated access point are allowed simultaneously etc. However, after the relevant security indication has been set, all traffic that should be dropped is dropped, and the packet on the secure PDP context is forwarded to the security indicated accesses point, 104. A timer is
15   started/restarted to establish when the security indication can be dropped, 105. This can be provided for in different manners, cf. Fig. 6C. The timer is thus started/restarted after each packet. Finally the procedure for that particular packet is finished.

20   Fig. 6B describes, for the dynamic enforcement, the case when a packet is incoming to an access point which is not security indicated. It should be clear that packets on an allowed PDP context e.g. MMS accept, do not affect the security indication, and they are also not affected thereby themselves.
25
It is supposed that a packet is detected on a PDP context to an access point which is not security indicated, 101A. An examination is then performed to establish whether a security indication is set to any related access point connection, 102A, if yes, the
30   packet dropped, 103A', and the procedure as far as this "non-secure" packet is concerned is terminated, 104A'. If however, it is established that there is no security indication set to any related access point connection, the packet is forwarded, 103A,

23

and the procedure is ended as far as the particular packet is concerned.

Fig. 6C illustrates the procedure when the timer is
5   started/restarted, 100B, when a secure packet is forwarded. When the timer expires, the security indication can be dropped, 101B. The indication is then removed, 102B, and traffic can again be forwarded on an access point which is not secure, 103B.

10 Fig. 7 is a flow diagram describing a first implementation of a static security enforcement mechanism. The procedure starts, 201, with the arrival of a request to activate a PDP context to a security indicated access point, 202. More generally it relates to the activation of an access point connection comprising a security
15 indicated APN as discussed above. It is then examined if there are any PDP context(s) which is/are already active and which would expose the security indicated access point, 203, or in other terms the security loophole. If yes, the request is rejected, 203A, and the procedure ends, 203B. If, however, there is no PDP context
20 which would interfere with or expose the security indicated access point, activation of new PDP contexts which would expose the security indicated access point is blocked, 204, and then the request is accepted, 205. Traffic is then exchanged on the secure PDP context to the security indicated access point, 206. When all
25 traffical packets of the secure PDP context have been sent, the security indicated PDP context is deactivated, 207, and activation of new PDP context is enabled, 208, whereafter the procedure ends for this PDP context to the security indicated access point, 209. This algorithm particularly requires that the end user himself
30 ensures that no conflicting PDP contexts are active when a new PDP context is requested to the security indicated access point, or APN. However, it could also be possible to implement some automatic detection of conflicting concurrent PDP contexts.

Fig. 8 shows another implementation of a static enforcement mechanism, the procedure starting, 301, with an activation of a PDP context to a security indicated access point, 302. Activation of new PDP contexts which would expose the security indicated access point are then blocked, 303. After that, as opposed to the embodiment as discussed with reference to Fig. 7, it is examined whether there is/are any PDP context(s) that already is/are active and which would expose the security indicated access point, 304. If yes, all PDP contexts exposing the security indicated access point are deactivated, 305. After that, or if there was no PDP context already active and which would expose the security indicated access point, traffic is exchanged on the secure PDP context to the security indicated access point, 306. When all traffic has been exchanged of the secure PDP context, the security indicated PDP context is deactivated, 307. Subsequently activation of new PDP contexts is enabled, 308, and the procedure ends, 309, for that PDP context incoming to a security indicated access point. In this procedure all conflicting PDP context are deactivated and have to be reactivated, e.g. by the end user, when they are needed again. It should be clear that all concurrent conflicting PDP contexts either means all other PDP contexts than a first PDP context incoming to a security indicated access point, or all other PDP contexts not fulfilling one or more criteria defining which PDP contexts are allowed to be active simultaneously.

Fig. 9 shows a third implementation of a static enforcement procedure starting, 401, when a packet is detected on a PDP context to a security indicated access point, 402. Activation of new PDP contexts which would expose the security indicated access point is blocked, 403. Then it is examined if there are any PDP contexts which would expose the security indicated access point

which already are active, 404. If yes, all PDP contexts (which are
not secure or allowed simultaneously) exposing the security
indicated access point are deactivated, 405. Then, and if there
was no already active PDP context that might expose the security
5   indicated access point, traffic is exchanged on the secure PDP
context to the security indicated access point, 406. When all the
traffic on the secure PDP context has been exchanged, the secure
PDP context is deactivated, 407, and activation of new PDP
contexts is enabled, 408. Thereafter the procedure comes to an
10 end, 409, for the packet detected on a PDP context to a security
indicated access point. This algorithm also results in all
conflicting PDP contexts being deactivated and having to be
reactivated again when needed, e.g. by the end user.

15 Fig. 10 most schematically illustrates the support of mobility
when an end user moves from the "coverage" of one SGSN (old SGSN)
to another SGSN (new SGSN). When the new SGSN sends a SGSN context
request to the old SGSN, the old SGSN responds with a SGSN context
response including the security indication as enforced in old
20 SGSN, cf. also Figs. 2A-2C.

In the application it has been referred to one or more criteria
that may be comprised by a security indication for allowing
"simultaneous" communication. One example on criteria is given in
25 the document S2-032971, CR on 23.060 as referred to earlier in the
application.

In that implementation an APN Restriction is associated to each
APN configured at the GGSN. It is used to relate PDP contexts
using a certain APN to the type of that APN, such as public access
30 or private corporate APN. It is further used to control the valid
combinations of PDP contexts that may be simultaneously active to
different APNs.

Then value 0 is may be allocated to a public-1 type of APN, with a typical end point WAP or MMS, value 1 assigned to a public-2 type of APN with a typical endpoint in Internet or PSPDN (Packet Switched Packet Data Network), value 2 is assigned to a private-1 type of APN with a typical endpoint at a corporate network (e.g. using MMS), whereas value 3 is assigned to a private-2 type of APN with an endpoint in a corporate network not using e.g. MMS. Valid combinations will then be for value 0: values 0,1,2; for value 1: values 0,1; for value 2: value 0; for value 3: none.

Value 3 may e.g. be used by government offices having the highest security requirements or other organizations or firms requiring such a high security.

During the PDP context activation procedure, the APN restriction value for the PDP context being set up may be used by the GGSN to control whether this activation is accepted, based on the most restrictive value of the APN restriction (maximum APN restriction) for the already active PDP contexts, if any, and the APN restriction for this activation. The APN restriction for this PDP context activation shall be transferred to the SGSN for storage.

The APN restriction for each PDP context, if available, shall be transferred from the GGSN to the new SGSN in inter-SGSN routing area updates. The new SGSN shall calculate the maximum APN restriction based on the most restrictive value of the APN restriction (maximum APN restriction) for the already active PDP contexts, if any. If the new SGSN detects that there are PDP contexts to different APNs that violate valid combinations based on the APN restriction, the resultant handling will be network operator dependent.

27

It should be clear that the invention is not limited to the specifically illustrated embodiments, but that it can be varied in a number of ways within the scope of the appended claims. It is e.g. applicable also for WLAN access. Then SGSN is replaced by a
5   WAG (WLAN Access Gateway) or a PDGN (Packet Data Gateway).